# CMSC 858L: Quantum Complexity

Instructor: Daniel Gottesman

Spring 2023

## 7 Matchgates

The analysis of matchgates is based on Terhal and DiVincenzo, "Classical simulation of noninteracting-fermion quantum circuits," quant-ph/0108010 and Jozsa and Miyake, "Matchgates and classical simulation of quantum circuits," arXiv:0804.4050 [quant-ph]. The result pinpointing the exact strength of matchgates is Jozsa, Kraus, Miyake, and Watrous, "Matchgate and space-bounded quantum computations are equivalent," arXiv:0908.1467 [quant-ph].

### 7.1 Finishing the Clifford group

This theorem about classical simulation of the Clifford group can be strengthened in a few different ways. First, note that the proof already shows that we don't need to have measurement only at the end of the computation. We can allow measurement in the middle of the computation and condition future unitaries on the result of some classical computation.

If we don't allow conditional unitaries and wish to solve a decision problem using only Clifford group gates, the above theorem tells us that the problem is in P. We might wonder if it can do all of P, or if it is located in some smaller complexity class. Indeed, Clifford group gates by themselves are *not* as strong as P. Instead, this problem is complete for a class called $\oplus$L, which is the set of problems reducible via a logspace reduction (not a polynomial-time reduction) to a sequence of XORs (i.e., CNOTs). Indeed, most of the algorithm to simulate a Clifford group circuit just involves XORs. The only place where we need more is in calculating the overall phases, which needs a very limited amount of mod4 arithmetic. However, this part can still be done as part of the logspace reduction.

Another practical impact of this theorem is that many algorithms for more-efficient-than-the-obvious (but still exponential) classical simulation of general quantum circuits build on it. For instance, there are algorithms that are exponential in the number of non-Clifford gates in the circuit, which can be very effective in simulating circuits which are mostly Clifford gates.

### 7.2 Matchgates

We now turn to a set of gates that has a somewhat different set of rules. We will still assume that we are starting in the state $|00\ldots0\rangle$ and measuring at the end in the computational basis, but now the qubits have an order and we can only perform gates on adjacent qubits. For the Clifford group, putting the qubits in a line like this wouldn't have mattered, because the SWAP gate is in the Clifford group, so we could reorder however we liked. The current set of gates won't quite have the SWAP gate, however.

The gates we are interested are the set of two-qubit gates of the form

$$G(A,B) = \begin{pmatrix} a & 0 & 0 & b \\ 0 & w & x & 0 \\ 0 & y & z & 0 \\ c & 0 & 0 & d \end{pmatrix}, \tag{1}$$

where

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, B = \begin{pmatrix} w & x \\ y & z \end{pmatrix} \tag{2}$$

are matrices in $SU(2)$. Recall that this means they are unitary and have determinant 1. Note that this is a case where it matters that they are in $SU(2)$ rather than $U(2)$ because it is important for the result that they have the same relative phase. So, for instance, the SWAP gate wouldn't work because it has the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \tag{3}$$

which would give us a $B$ with determinant $-1$. Instead we can have an "iSWAP" gate

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \tag{4}$$

which swaps the two qubits but creates a phase $i$ if they are not the same.

These gates, the *matchgates*, rotate adjacent pairs of qubits in the $|00\rangle$ and $|11\rangle$ subspace and the $|01\rangle$ and $|10\rangle$ subspace. Thus, they preserve the total parity of the state. There is also some phase constraint to the rotation, as we saw with the SWAP/iSWAP example. They have a physical interpretation as beam splitters and pair creation/destruction for non-interacting Majorana fermions. (Note: the original paper about classical simulation of matchgates by Valiant had some additional non-unitary gates, but these are not too relevant for most quantum computing applications.)

Note that matchgates include the identity and all single-qubit phase gates (with suitable global phase), but not things like the single-qubit Hadamard or bit flip. This is an infinite set, however, unlike the Clifford group. To restrict it to a reasonable complexity class, we should require that the matrices $A$ and $B$ are efficiently computable.

Leaning into the interpretation of Majorana fermions (and if you don't know what they are, that's OK, but it provides motivation), we can define the Majorana operators from the Paulis via the *Jordan-Wigner* transformation:

$$c_1 = X_0,\ c_2 = Y_0,\ c_{2i+1} = \bigotimes_{j=0}^{i-1} Z_j X_i,\ c_{2i+2} = \bigotimes_{j=0}^{i-1} Z_j Y_i \tag{5}$$

for $i = 1, \ldots, n-1$. Thus, there are $2n$ operators $c_\mu$ for $n$ qubits.

**Theorem 1.** *For any matchgate $G(A,B)$, for all $\mu$*

$$G(A,B)^\dagger\, c_\mu\, G(A,B) = \sum_\nu R_{\mu\nu} c_\nu. \tag{6}$$

*Proof.* One way to show this is to first note that any matchgate $G(A,B) = e^{-iH}$, where $H$ is a sum of terms quadratic in the $c$'s. This in turn will imply the result.

However, it is fairly straightforward and more elementary to just calculate this. First note that since $G(A,B)$ is a 2-qubit gate, we only need focus attention on two adjacent qubits in $c_\mu$, and there are only 6 possible 2-qubit Paulis that appear on adjacent qubits in any $c_\mu$: $I \otimes I$, $Z \otimes Z$, $X \otimes I$, $Y \otimes I$, $Z \otimes X$, and $Z \otimes Y$.

Now, $I \otimes I$ commutes with anything, so $G(A,B)^\dagger (I \otimes I) G(A,B) = I \otimes I$. $Z \otimes Z$ acts like $I$ on the $|00\rangle$, $|11\rangle$ subspace and like $-I$ on the $|01\rangle$, $|10\rangle$ subspace, so again it commutes with $G(A,B)$ (which doesn't mix those subspaces): $G(A,B)^\dagger (Z \otimes Z) G(A,B) = Z \otimes Z$. Thus, if $G(A,B)$ acts on qubits $i$ and $i+1$, all of the $c_\mu$ with $\mu < 2i+1$ or $\mu > 2i+4$ are left unchanged by conjugation.

That leaves $X \otimes I$ (which is $c_{2i+1}$ on qubits $i$ and $i+1$), $Y \otimes I$ (which is $c_{2i+2}$), $Z \otimes X$ ($c_{2i+3}$), and $Z \otimes Y$ ($c_{2i+4}$). We will show that conjugation gives us a linear combination of these same four operators.

First, observe:

$$X \otimes I = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{7}$$

$$Y \otimes I = \begin{pmatrix} 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \end{pmatrix} \tag{8}$$

$$Z \otimes X = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \tag{9}$$

$$Z \otimes Y = \begin{pmatrix} 0 & 0 & -i & 0 \\ 0 & 0 & 0 & i \\ i & 0 & 0 & 0 \\ 0 & -i & 0 & 0 \end{pmatrix}. \tag{10}$$

Then we can calculate $G(A,B)^\dagger (X \otimes I) G(A,B)$:

$$G(A,B)^\dagger (X \otimes I) G(A,B) = \begin{pmatrix} a^* & 0 & 0 & c^* \\ 0 & w^* & y^* & 0 \\ 0 & x^* & z^* & 0 \\ b^* & 0 & 0 & d^* \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} a & 0 & 0 & b \\ 0 & w & x & 0 \\ 0 & y & z & 0 \\ c & 0 & 0 & d \end{pmatrix} \tag{11}$$

$$= \begin{pmatrix} 0 & a^*w + c^*y & a^*x + c^*z & 0 \\ aw^* + cy^* & 0 & 0 & bw^* + dy^* \\ ax^* + cz^* & 0 & 0 & bx^* + dz^* \\ 0 & b^*w + d^*y & b^*x + d^*z & 0 \end{pmatrix}. \tag{12}$$

Now, this has 0s in the right place and is Hermitian, but in order for it to be correct, we need some relationship between the top left and bottom right blocks and the top right and bottom left blocks. This follows because $A$ and $B$ are in $SU(2)$.

In particular, for a unitary matrix, the rows and columns must be orthonormal vectors, and for a 2-D Hilbert space, that is very limiting, and even more so for an element of $SU(2)$. In particular, $A$ must have the form

$$A = \begin{pmatrix} a & b \\ -b^* & a^* \end{pmatrix} \tag{13}$$

and

$$B = \begin{pmatrix} w & x \\ -x^* & w^* \end{pmatrix}. \tag{14}$$

This tells us

$$a^*w + c^*y = a^*w + bx^* = bx^* + dz^* \equiv r + is \tag{15}$$

$$a^*x + c^*z = a^*x - bw^* = -(bw^* + dy^*) \equiv t + iu \tag{16}$$

with real $r, s, t, u$. Thus,

$$G(A,B)^\dagger (X \otimes I) G(A,B) = \begin{pmatrix} 0 & r+is & t+iu & 0 \\ r-is & 0 & 0 & -t-iu \\ t-iu & 0 & 0 & r+is \\ 0 & -t+iu & r-is & 0 \end{pmatrix} \tag{17}$$

$$= rX \otimes I - sY \otimes I + tZ \otimes X - uZ \otimes Y. \tag{18}$$

Similarly for the other three cases. □

As a consequence of this theorem, we can immediately track the behavior of any matchgate circuit by following the evolution of the $c_\mu$'s. Note that since there are only $2n$ $c_\mu$'s, $R_{\mu\nu}$ is a $2n \times 2n$ matrix, so we can store it classically and multiply the $R$ matrices corresponding to each matchgate in the circuit. This gives us an overall $R$ matrix that determines the behavior of the circuit.

But once again, this is not enough. We need to determine measurement outcomes. To do so, note that $Z_i = -ic_{2i+1}c_{2i+2}$. Then if $|\psi\rangle = U|00\ldots0\rangle$ for some $U$ corresponding to a matchgate circuit with overall matrix $R$,

$$\langle\psi|Z_i|\psi\rangle = -i\langle 00\ldots0|U^\dagger c_{2i+1}c_{2i+2}U|00\ldots0\rangle \tag{19}$$

$$= -i\langle 00\ldots0|(U^\dagger c_{2i+1}U)(U^\dagger c_{2i+2}U)|00\ldots0\rangle \tag{20}$$

$$= -i\sum_{\nu,\xi} R_{2i+1,\nu}R_{2i+2,\xi}\langle 00\ldots0|c_\nu c_\xi|00\ldots0\rangle. \tag{21}$$

Now, $c_\nu c_\xi$ can be translated back as a product of Paulis $\bigotimes P_i$, so

$$\langle 00\ldots0|c_\nu c_\xi|00\ldots0\rangle = \prod_i \langle 0|P_i|0\rangle. \tag{22}$$

Since $\langle\psi|Z_i|\psi\rangle = \text{Prob}(0) - \text{Prob}(1)$ when qubit $i$ is measured in the standard basis, we can therefore efficiently calculate the measurement distribution on qubit $i$. Given a circuit of $T$ matchgates, the procedure involves multiplying $T$ $2n \times 2n$ matrices to find $R$ and then summing up potentially $O(n^2)$ terms, each of which can be computed in time $O(n)$.

The marginal probability of getting outcome $v$ on some subset of qubits is

$$\text{Prob}(v) = \text{Tr}(|v\rangle\langle v|)|\psi\rangle\langle\psi| \tag{23}$$

We can write the projector on $|v\rangle$ in terms of the $c_\mu$ as well, and then calculate this using the same procedure as above. However, the time to do this calculation is exponential in the number of $c$'s, which is proportional to the number of qubits whose joint measurement we are simulating, so this approach is inherently limited.

Nevertheless, it is possible to do so using a more sophisticated argument (which I will not reproduce). The answer turns out to be the Pfaffian of some $n \times n$ matrix, and the Pfaffian is the square root of the determinant, and so can be computed in polynomial time (for instance by diagonalizing the matrix).

Joint measurement of subsets then gives us conditional probability distributions:

$$\text{Prob}(0|v) = \text{Prob}(0v)/\text{Prob}(v). \tag{24}$$

Therefore, we have the following result:

**Theorem 2.** *There is an efficient classical algorithm to perform an exact strong simulation of any circuit of matchgates specified with constant precision.*

There are also various strengthenings of this result. For instance, the exact power of matchgates (at least for decision problems) is known: The class of decision problems solvable with bounded probability with matchgates is equivalent (under classical logspace reductions) to logspace quantum computation.